Commonwealth of Massachusetts
Center for Health Information & Analysis (CHIA)
Non-Government Agency Application for Data

This application is to be used by all applicants, except Government Agencies, as defined in 957 CMR 5.02.

***NOTE*: In order for your application to be processed, you must submit the required application fee. Please consult the fee schedules for APCD and Case Mix data for the appropriate fee amount. A remittance form with instructions for submitting the application fee is available on the CHIA website.**

I. GENERAL INFORMATION

APPLICANT INFORMATION	
Applicant Name:	
Title:	
Organization:	
Project Title:	
Date of Application:	
Project Objectives (240 character limit)	
Project Research Questions (if applicable)	1. 2. 3.

Please indicate if you are a Researcher, Payer, Provider, Provider Organization or Other entity and whether you are seeking data pursuant to 957 CMR 5.04 (De-Identified Data), 957 CMR 5.05 (Direct Patient Identifiers for Treatment or Coordination of Care), or 957 CMR 5.06 (Discretionary Release).

□ Researcher	□ 957 CMR 5.04 (De-identified Data)
□ Payer	□ 957 CMR 5.05 (Direct Patient Identifiers)
□ Provider / Provider Organization	□ 957 CMR 5.06 (Discretionary Release)
□ Other	

II. PROJECT SUMMARY

Briefly describe the purpose of your project and how you will use the requested CHIA data to accomplish your purpose.

III. FILES REQUESTED

Please indicate the databases from which you seek data, the Level(s) and Year(s) of data sought.

ALL PAYER CLAIMS DATABASE	Level 1[1] or 2[2]	Single or Multiple Use	Year(s) Of Data Requested Current Yrs. Available 2009 - 2012
□ Medical Claims	□ Level 1 □ Level 2	Multiple ▾	□ 2009 □ 2010 □ 2011 □ 2012
□ Pharmacy Claims	□ Level 1 □ Level 2	▾	□ 2009 □ 2010 □ 2011 □ 2012
□ Dental Claims	□ Level 2	Select... ▾	□ 2009 □ 2010 □ 2011 □ 2012
□ Member Eligibility	□ Level 2	Select... ▾	
□ Provider	□ Level 2	Select... ▾	
□ Product	□ Level 2	Select... ▾	

CASEMIX	Level 1 - 6	Fiscal Years Requested
Inpatient Discharge	□ Level 1 – No Identifiable Data Elements □ Level 2 – Unique Physician Number (UPN) □ Level 3 – Unique Health Information Number (UHIN) □ Level 4 – UHIN and UPN □ Level 5 – Date(s) of Admission; Discharge; Significant Procedures □ Level 6 – Date of Birth; Medical Record Number; Billing Number	1998-2012 Available (limited data 1989-1997)
Outpatient Observation	□ Level 1 – No Identifiable Data Elements □ Level 2 – Unique Physician Number (UPN) □ Level 3 – Unique Health Information Number (UHIN) □ Level 4 – UHIN and UPN □ Level 5 – Date(s) of Admission; Discharge; Significant Procedures □ Level 6 – Date of Birth; Medical Record Number; Billing Number	2002-2012 Available
Emergency Department	□ Level 1 – No Identifiable Data Elements □ Level 2 – Unique Physician Number (UPN)	2000-2012 Available

[1] Level 1 Data: De-identified data containing information that does not identify an individual patient and with respect to which there is no reasonable basis to believe the data can be used to identify an individual patient. This data is de-identified using standards and methods required by HIPAA.

[2] Level 2 (and above) Data: Includes those data elements that pose a risk of re-identification of an individual patient.

	□ Level 3 – Unique Health Information Number (UHIN) □ Level 4 – UHIN and UPN; Stated Reason for Visit □ Level 5 – Date(s) of Admission; Discharge; Significant Procedures □ Level 6 – Date of Birth; Medical Record Number; Billing Number	

IV. FEE INFORMATION

Please consult the fee schedules for APCD (Administrative Bulletin 13-11) and Case Mix data (Administrative Bulletin 13-09) and select from the following options:

APCD Applicants Only

□ Academic Researcher
□ Others (Single Use)
□ Others (Multiple Use)

Case Mix Applicants Only

□ Single Use
□ Limited Multiple Use
□ Multiple Use

Are you requesting a fee waiver?

□ Yes
□ No

If yes, please submit a letter stating the basis for your request.

V. REQUESTED DATA ELEMENTS [APCD Only]

State and federal privacy laws limit the use of individually identifiable data to the minimum amount of data needed to accomplish a specific project objective. Please use the APCD Data Specification Workbook to identify which data elements you would like to request and attach this document to your application.

VI. MEDICAID DATA [APCD Only]

Please indicate here whether you are seeking Medicaid Data:

□ Yes
□ No

Federal law (42 USC 1396a(a)7) restricts the use of individually identifiable data of Medicaid recipients to uses that are directly connected with the administration of the Medicaid program. If you are requesting Medicaid data from Level 2 or above, please describe in detail why your use of the data meets this requirement. Applications requesting Medicaid data will be forwarded to MassHealth for a determination as to whether the proposed use of the data is directly connected to the administration of the Medicaid program. MassHealth may impose additional requirements on applicants for Medicaid data as necessary to ensure compliance with federal laws and regulations regarding Medicaid.

VII. MEDICARE DATA

Please indicate here whether you are seeking Medicare Data:

☐ Yes
☐ No

Medicare data may only be disseminated to state agencies and/or entities conducting research projects that are directed and partially funded by the state if such research projects would allow for a Privacy Board or an IRB to make the findings listed at 45 CFR 164.512(i)(2)(ii) if the anticipated data recipient were to apply for the data from CMS directly. If you are requesting Medicare data, please explain how your research project is directed and partially funded by the state and describe in detail why your proposed project meets the criteria set forth in 45 CFR 164.512(i)(2)(ii). Applicants must describe how they will use the data and inform CHIA where the data will be housed. CHIA must be informed if the data has been physically moved, transmitted, or disclosed.

Applicants seeking Medicare data must complete a Medicare Request Form.

Applicants approved to receive Medicare data will be required to execute an Addendum to CHIA's standard data use agreement, containing terms and conditions required by CHIA's data use agreement with CMS.

VIII. DIRECT PATIENT IDENTIFIERS[3]

State and federal privacy laws may require the consent of Data Subjects prior to the release of any Direct Patient Identifiers. If you are requesting data that includes Direct Patient Identifiers, please provide documentation of patient consent or your basis for asserting that patient consent is not required.

IX. REQUESTS PURSUANT TO 957 CMR 5.04

Payers, providers, provider organizations and researchers seeking access to Level 1 (de-identified) data are required to describe how they will use such data for the purposes of lowering total medical expenses, coordinating care, benchmarking, quality analysis or other administrative research purposes. Please provide this information below.

[3] Direct Patient Identifiers. Personal information, such as name, social security number, and date of birth, that uniquely identifies an individual or that can be combined with other readily available information to uniquely identify an individual.

X. FILTERS

If you are requesting APCD elements from Level 2 or above, describe any filters you are requesting to use in order to limit your request to the minimum set of records necessary to complete your project. (For example, you may only need individuals whose age is less than 21, claims for hospital services only, or only claims from small group projects.)

APCD FILE	DATA ELEMENT(S) FOR WHICH FILTERS ARE REQUESTED	RANGE OF VALUES REQUESTED
Medical Claims		
Pharmacy Claims		
Dental Claims		
Membership Eligibility		
Provider		
Product		

XI. PURPOSE AND INTENDED USE

1. Please explain why completing your project is in the public interest.

2. **Attach** a brief (1-2 pages) description of your research methodology. (This description will not be posted on the internet.)

3. Has your project received approval from your organization's Institutional Review Board (IRB)?

   □ Yes, and a copy of the approval letter is attached to this application.

   □ No, the IRB will review the project on ______________________.

   □ No, this project is not subject to IRB review.

   □ No, my organization does not have an IRB.

XII. APPLICANT QUALIFICATIONS

1. Describe your qualifications to perform the research described or accomplish the intended use of CHIA data.

2. Attach résumés or curriculum vitae of the applicant/principal investigator, key contributors, and of all individuals who will have access to the data. (These attachments will not be posted on the internet.)

XIII. DATA LINKAGE AND FURTHER DATA ABSTRACTION

1. Does your project require linking the CHIA Data to another dataset?

   □ Yes
   □ No

2. If yes, will the CHIA Data be linked to other patient level data or with aggregate data (e.g. Census data)?

   □ Patient Level Data
   □ Aggregate Data

3. If yes, please identify all linkages proposed and explain the reasons(s) that the linkage is necessary to accomplish the purpose of the project.

4. If yes, please identify the specific steps you will take to prevent the identification of individual patients in the linked dataset.

XIV. PUBLICATION / DISSEMINATION / RE-RELEASE

1. Describe your plans to publish or otherwise disclose CHIA Data, or any data derived or extracted from such data, in any paper, report, website, statistical tabulation, seminar, conference, or other setting.

2. Will the results of your analysis be publicly available to any interested party? Please describe how an interested party will obtain your analysis and, if applicable, the amount of the fee.

3. Will you use the data for consulting purposes?

   □ Yes
   □ No

4. Will you be selling standard report products using the data?

   □ Yes
   □ No

5. Will you be selling a software product using the data?

   □ Yes
   □ No

6. If you have answered “yes” to questions 3, 4 or 5, please describe the types of products, services or studies.

XV. USE OF AGENTS AND/OR CONTRACTORS

Third-Party Vendors. Provide the following information for all agents and contractors who will work with the CHIA Data.

Company Name:	
Contact Person:	
Title:	
Address:	
Telephone Number:	
E-mail Address:	
Organization Website:	

7. Will the agent/contractor have access to the data at a location other than your location or in an off-site server and/or database?

   ☐ Yes
   ☐ No

8. Describe the tasks and products assigned to this agent or contractor for this project.

9. Describe the qualifications of this agent or contractor to perform such tasks or deliver such products.

10. Describe your oversight and monitoring of the activity and actions of this agent or subcontractor.

Information provided from this page forward will NOT be posted publicly on the internet.

XVI. APPLICANT CONTACT INFORMATION

Applicant Name:	
Title:	
Organization:	
Address:	
Telephone Number:	
E-mail Address:	
E-mail Addresses of ALL Co-Investigators:	

XVII. DATA SECURITY AND INTEGRITY

(Information provided in this section is confidential and not a public record.)
Complete this section for each location where the data will be stored or accessed. If you plan to use an agent/contractor that has access to the data at a location other than your location or in an off-site server and/or database, the agent/contractor should complete this section.

1. *Physical Location of the data*: Please provide the delivery address for the data, as well as the full address, including building and floor, of each location where data will be stored.

2. *Person Responsible for securing the data:* Please provide the name and contact information of the individual responsible for securing the data.

3. *Data Privacy Training and Awareness:* Has every individual who will access the data received training on the proper handling of protected health information and/or personal data within the last two (2) years? If so, please provide the name of the training event, location where given, and who provided it (name of the instructor or sponsor).

4. *Encryption of copied data:* Will the APCD data or any copy of the data be copied from the encrypted hard drive to another storage medium? If yes, is the storage medium encrypted? With what level of encryption (e.g., AES 256 bit)?

5. *Software Applications Accessing the Data:* What is the provider (company, etc.), product name, and version of the software application used to access and manipulate the data? If this software application is a *custom* application (i.e., developed in-house or by a third party specifically for your organization) then attach all development documentation relevant to its authorization, authentication, and other security features and capabilities (functional specification(s), security design review, security architecture and workflow diagrams, security test plan(s), security code review(s), etc.).

6. *Technical Safeguards*: What additional specific technical safeguards (not mentioned in prior answers) will be used to *mitigate* the risk of unauthorized access to each of the following:

a) The original data media and subsequent copies of the data, including backups of the data.

b) Any work, scratch, or temporary files generated from the data.

c) Any device (appliances, workstations, servers, et al) with Internet connectivity which can also connect internally to any other device containing the data or a copy of the data.

7. *Portable Computing Devices*: How will you prevent *all* portable computing devices (laptops, tablets, notebooks, netbooks, smartphones et al), whether owned or issued by your organization or other parties or persons, from gaining access to, or storing, the data or copies of the data?

8. *Administrative Safeguards*: If your agency has a Written Information Security Program (WISP) or information security policy(ies) that contains data security provisions, please attach the document(s) and refer to the applicable sections in your response to the questions below.

9. List any additional technical information security or privacy safeguards your organization has pertinent to mitigating the risk of unauthorized access to or use of the data.

10. *Enterprise Information Security* (to be completed by an employee responsible for Information Security in the organization):

a. Name: ____

b. Title: ____

c. Has every individual who will access the data received training on their user cyber security responsibilities within the last two (2) years [Y/N]? If so, please provide the name of the training event, location where given, and who provided it (name of the instructor or sponsor):

____

d. Has your organization had a breach of PHI or PII in the last seven (7) years [Y/N]? If yes, then what was the resolution? ____

e. On the system that will access the data, is an audit log maintained of all user logons to the system [Y/N]? How many days of activity are preserved in the log? _________

f. Are all the user accounts that log on to any machine (server or endpoint) that accesses the data uniquely assigned to individual users (i.e., the user accounts are not shared)? [Y/N]

g. What is the minimum password length and character complexity (uppercase, lowercase, numeric, and special characters) required for new passwords on the user accounts logging on to the system accessing the APCD data? ________________________

h. Do you run an anti-virus or anti-malware product on the server that will host the data [Y/N]? If Yes, is the software at a current patch/revision/version level? If no, what is the product name and patch/revision/version number? ____

i. Check all the security features of the room containing the server hosting the APCD data or a copy of it:

i. □ Continuous live recorded video with server in field view

ii. □ Access log of all individuals entering the room

iii. □ Secure server rack

iv. □ Locked room

j. When was the last information security risk assessment performed in your enterprise? Who conducted it? ____

k. When was the last IT audit performed in your enterprise? Who conducted it?

____

XVIII. DATA RETURN OR DESTRUCTION

Applicants are required to attest that the original released CHIA Data and all copies of the CHIA Data used by the Applicant or its employees, contractors or agents will be destroyed upon completion of the project described in this Application. All data destruction must conform to the requirements of M.G.L. c. 93I. Specify the measures you will use to meet these requirements.

XIX. ASSURANCES

Applicants requesting and receiving data from CHIA pursuant to 957 CMR 5.00 ("Data Recipients") will be provided with data following the execution of a data use agreement that requires the Data Recipient to adhere to processes and procedures aimed at preventing unauthorized access, disclosure or use of data.

Data Recipients are further subject to the requirements and restrictions contained in applicable state and federal laws protecting privacy and data security, including but not limited to the Massachusetts Fair Information Practices Act, M.G.L. c. 66A; M.G.L. c. 93H (data breaches); and M.G.L. c. 93I (data destruction).

Data Recipients must notify CHIA of any unauthorized use or disclosure of CHIA data.

Signature:	
Printed Name:	
Title:	
Agency:	
Date:	